PATENT ABSTRACTS OF JAPAN

(11)Publication number : **11-065934**
(43)Date of publication of application : **09.03.1999**

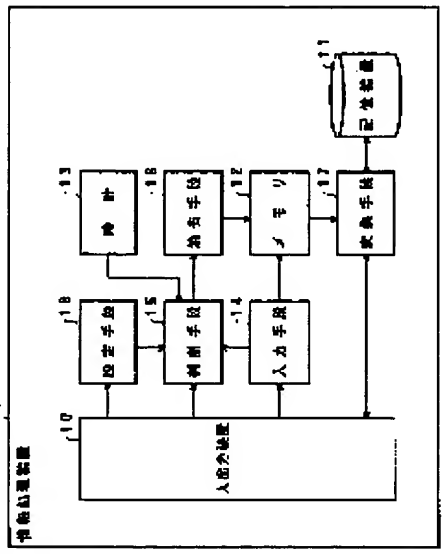
(51)Int.Cl. **G06F 12/14**

(21)Application number : **09-219388**
(22)Date of filing : **14.08.1997**

(71)Applicant : **FUJITSU LTD**
(72)Inventor : **MATSUNAGA RYOTARO**
SAITO TADASHI

(54) INFORMATION PROCESSOR AND PROGRAM STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To improve operability while holding secrecy by receiving and storing a cryptographic key in a memory, confirming the lapse of a normalized time from the input point of time of the cryptographic key, and decoding the secret information by the cryptographic key held in the memory.
SOLUTION: An inputting means 14 receives a cryptographic key inputted from an inputting and outputting device 10, and stores it in a memory 12. A judging means 15 judges whether or not a normalized time passes since the input point of time of the cryptographic key of the inputting means 14, and judges whether or not the normalized time passes since the inputting operation of the inputting and outputting device 10 stops. A converting means 17 decodes secret information stored in a storage device 11 into a sentence by using the cryptographic key held in the memory 12, and enciphers the secret information of the sentence edited by the inputting and outputting device 10. The normalized time to be used for the processing of a judging means 15 is set by a setting means 18. Thus, the decoding and encipherment of the secret information can be attained without inputting any cryptographic key while the cryptographic key is held in the memory 12, and operability can be improved while secrecy is maintained.



LEGAL STATUS

[Date of request for examination] 29.07.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平11－65934

(43)公開日　平成11年(1999)３月９日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ
			３２０Ｆ

審査請求　未請求　請求項の数７　ＯＬ　（全 14 頁）

(21)出願番号　特願平9－219388

(22)出願日　平成９年(1997)８月14日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　松永　良太郎
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　斉藤　紀
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(74)代理人　弁理士　岡田　光由　（外１名）

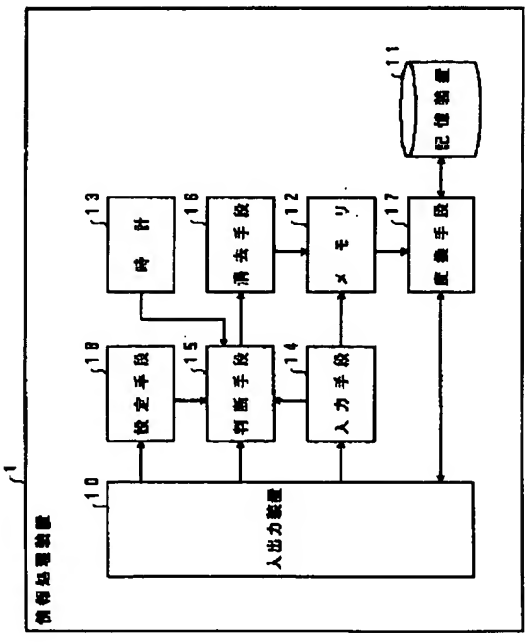
(54)【発明の名称】　情報処理装置及びプログラム記憶媒体

(57)【要約】

【課題】本発明は、機密情報の機密性を維持しつつ、操作性の向上を実現する情報処理装置の提供を目的とする。

【解決手段】入力装置と、暗号化された機密情報を記憶する記憶装置とを備える情報処理装置において、入力装置から入力される暗号鍵を受け取ってメモリに格納する入力手段１４と、入力手段１４による暗号鍵の入力時点から規定時間が経過したのか否かを判断する判断手段１５と、判断手段１５が時間経過を判断するときに、メモリに保持される暗号鍵を消去する消去手段１６と、メモリに保持される暗号鍵を用いて、記憶装置の記憶する機密情報を平文に復号化する変換手段１７とを備えるように構成する。

本発明の原理構成図



1

【特許請求の範囲】
【請求項１】　入力装置と、暗号化された機密情報を記憶する記憶装置とを備える情報処理装置において、
入力装置から入力される暗号鍵を受け取ってメモリに格納する入力手段と、
上記入力手段による暗号鍵の入力時点から規定時間が経過したのか否かを判断する判断手段と、
上記判断手段が時間経過を判断するときに、上記メモリに保持される暗号鍵を消去する消去手段と、
上記メモリに保持される暗号鍵を用いて、記憶装置の記憶する機密情報を平文に復号化する変換手段とを備えることを、
特徴とする情報処理装置。
【請求項２】　入力装置と、暗号化された機密情報を記憶する記憶装置とを備える情報処理装置において、
入力装置から入力される暗号鍵を受け取ってメモリに格納する入力手段と、
上記入力装置の操作が途絶えてから規定時間が経過したのか否かを判断する判断手段と、
上記判断手段が時間経過を判断するときに、上記メモリに格納される暗号鍵を消去する消去手段と、
上記メモリに保持される暗号鍵を用いて、記憶装置の記憶する機密情報を平文に復号化する変換手段とを備えることを、
特徴とする情報処理装置。
【請求項３】　請求項１又は２記載の情報処理装置において、
変換手段は、入力装置により編集される平文の機密情報を、メモリに保持される暗号鍵を用いて暗号化することを、
特徴とする情報処理装置。
【請求項４】　請求項１ないし３記載の情報処理装置において、
対話処理に従って、判断手段の処理で用いられる規定時間を設定する設定手段を備えることを、
特徴とする情報処理装置。
【請求項５】　請求項１ないし４記載の情報処理装置において、
入力手段は、入力される暗号鍵の正当性をチェックして、正当な暗号鍵であることを条件にしてメモリに格納することを、
特徴とする情報処理装置。
【請求項６】　入力装置と、暗号化された機密情報を記憶する記憶装置とを備える情報処理装置の実現に用いられるプログラムが記憶されるプログラム記憶媒体であって、
入力装置から入力される暗号鍵を受け取ってメモリに格納する入力処理と、
上記入力処理による暗号鍵の入力時点から規定時間が経過したのか否かを判断する判断処理と、

2

上記判断処理が時間経過を判断するときに、上記メモリに保持される暗号鍵を消去する消去処理と、
上記メモリに保持される暗号鍵を用いて、記憶装置の記憶する機密情報を平文に復号化する変換処理とをコンピュータに実行させるプログラムが記憶されることを、
特徴とするプログラム記憶媒体。
【請求項７】　入力装置と、暗号化された機密情報を記憶する記憶装置とを備える情報処理装置の実現に用いられるプログラムが記憶されるプログラム記憶媒体であって、
入力装置から入力される暗号鍵を受け取ってメモリに格納する入力処理と、
上記入力装置の操作が途絶えてから規定時間が経過したのか否かを判断する判断処理と、
上記判断処理が時間経過を判断するときに、上記メモリに格納される暗号鍵を消去する消去処理と、
上記メモリに保持される暗号鍵を用いて、記憶装置の記憶する機密情報を平文に復号化する変換処理とをコンピュータに実行させるプログラムが記憶されることを、
特徴とするプログラム記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、暗号化された機密情報を記憶する情報処理装置と、その情報処理装置の実現に用いられるプログラムが記憶されるプログラム記憶媒体とに関し、特に、機密情報の機密性を維持しつつ、操作性の向上を実現する情報処理装置と、その情報処理装置の実現に用いられるプログラムが記憶されるプログラム記憶媒体とに関する。
【０００２】情報処理装置では、機密情報を取り扱う場合、漏洩を防ぐために機密情報を暗号化する構成を採っている。最近普及しつつある小型携帯端末でも、端末の紛失や盗難により機密情報の漏洩の危険度が高いことから、機密情報を暗号化する構成を採っている。
【０００３】一方、機密情報を暗号化する構成を採ると、その復号化に必要となる暗号鍵の入力をユーザに強いることになる。この暗号鍵の入力は、操作性の悪化をもたらす。これから、機密情報の機密性を維持しつつ、操作性の向上を実現する新たな情報処理装置を構築していく必要がある。
【０００４】
【従来の技術】情報処理装置は、機密情報のファイルを扱う場合、機密性を実現するために、その機密情報を暗号化するとともに、ファイルに、その暗号化に用いた暗号鍵を登録する構成を採っている。
【０００５】そして、暗号化された機密情報の参照を要求するユーザに対して、暗号鍵の入力を要求する構成を採って、ユーザから暗号鍵を指定して機密情報の参照が発行されると、ユーザから入力される暗号鍵と、ファイルに登録される暗号鍵とが一致するのか否かをチェック

して、一致することを判断するときには、ファイルに登録される暗号鍵を使って、ファイルの機密情報を復号化していくという構成を採っている。

【０００６】そして、ユーザが復号化された機密情報を編集した後に、それを再び暗号化してファイルに記憶することを要求する場合には、ユーザに対して、暗号鍵の入力を要求する構成を採って、ユーザから暗号鍵を指定して機密情報の暗号化要求が発行されると、ユーザから入力される暗号鍵と、ファイルに登録される暗号鍵とが一致するのか否かをチェックして、一致することを判断するときには、ファイルに登録される暗号鍵を使って、機密情報を暗号化してファイルに格納していくという構成を採っている。

【０００７】この構成を採るときに、従来では、機密情報の機密性を維持するという立場から、ユーザに対して、機密情報の参照要求の度に、暗号鍵を入力させていくとととともに、機密情報の暗号化要求の度に、暗号鍵を入力させていくという構成を採っていた。

【０００８】

【発明が解決しようとする課題】しかしながら、このような従来技術に従っていると、ユーザは、暗号化された機密情報を格納するファイルを操作する度に、その都度、暗号鍵を入力しなければならず、操作が繁雑になるという問題点があった。

【０００９】この操作を嫌って、機密情報の暗号化を怠ると、機密情報が漏洩する危険度が高くなるという問題点がある。特に、最近普及しつつある小型携帯端末は、作業場所が限定されないという利点がある一方で、第三者により不正に操作されることが起こり、この危険度は極めて高くなる。

【００１０】本発明はかかる事情に鑑みてなされたものであって、暗号化された機密情報を記憶する構成を採るときにあって、機密情報の機密性を維持しつつ、操作性の向上を実現する新たな情報処理装置の提供と、その情報処理装置の実現に用いられるプログラムが記憶される新たなプログラム記憶媒体の提供とを目的とする。

【００１１】

【課題を解決するための手段】図１に本発明の原理構成を図示する。図中、１は本発明を具備する情報処理装置であって、暗号化された機密情報を扱うものである。

【００１２】本発明の情報処理装置１は、入出力装置１０と、記憶装置１１と、メモリ１２と、時計１３と、入力手段１４と、判断手段１５と、消去手段１６と、変換手段１７と、設定手段１８とを備える。

【００１３】この入出力装置１０は、ユーザとの対話手段となる。記憶装置１１は、暗号化された機密情報を記憶する。メモリ１２は、暗号鍵を一時的に保持する。時計１３は、時刻情報を刻む。

【００１４】入力手段１４は、入出力装置１０から入力される暗号鍵を受け取ってメモリ１２に格納する。このとき、入力手段１４は、入力される暗号鍵の正当性をチェックして、正当な暗号鍵であることを条件にしてメモリ１２に格納することがある。判断手段１５は、入力手段１４による暗号鍵の入力時点から規定時間が経過したのか否かを判断したり、入出力装置１０で操作される入力操作が途絶えてから規定時間が経過したのか否かを判断する。

【００１５】消去手段１６は、メモリ１２に保持される暗号鍵を消去する。変換手段１７は、メモリ１２に保持される暗号鍵を用いて、記憶装置１１の記憶する機密情報を平文に復号化したり、入出力装置１０により編集される平文の機密情報を暗号化する。設定手段１８は、対話処理に従って、判断手段１５の処理で用いられる規定時間を設定する。

【００１６】ここで、本発明の情報処理装置１の持つ機能は具体的にはプログラムで実現されるものであり、このプログラムは、フロッピィディスクなどに記憶されたり、サーバなどのディスクなどに記憶され、それらから情報処理装置１にインストールされてメモリ上で動作することで、本発明を実現することになる。

【００１７】このように構成される本発明の情報処理装置１では、入力手段１４が入出力装置１０から入力される暗号鍵を受け取ってメモリ１２に格納すると、判断手段１５は、時計１３の時刻情報を参照することで、その暗号鍵の入力時点から、設定手段１８により設定される規定時間が経過したのか否かを判断し、この判断結果を受けて、消去手段１６は、判断手段１５が時間経過を判断するときに、メモリ１２に保持される暗号鍵を消去する。

【００１８】また、このように構成される本発明の情報処理装置１では、入力手段１４が入出力装置１０から入力される暗号鍵を受け取ってメモリ１２に格納すると、判断手段１５は、時計１３の時刻情報を参照することで、入出力装置１０で操作される入力操作が途絶えてから、設定手段１８により設定される規定時間が経過したのか否かを判断し、この判断結果を受けて、消去手段１６は、判断手段１５が時間経過を判断するときに、メモリ１２に保持される暗号鍵を消去する。

【００１９】このように、本発明の情報処理装置１では、ユーザの入力する暗号鍵が一定時間だけメモリ１２に保持され、その後、自動的に消去される構成が採られることで、この暗号鍵がメモリ１２に保持されている間は、ユーザは暗号鍵を入力することなく暗号化された機密情報を平文化できるとともに、平文化された機密情報を暗号化できることから、機密情報の機密性を維持しつつ、操作性の向上を実現できるようになる。

【００２０】

【発明の実施の形態】以下、実施の形態に従って本発明を詳細に説明する。図２に、本発明の情報処理装置の一実施例を図示する。

【００２１】この実施例に従う本発明の情報処理装置１は、入出力装置１０と、記憶装置１１と、消去時間設定プログラム２０と、設定時間格納域２１と、暗号鍵入力消去プログラム２２と、暗号鍵格納域２３と、暗号復号化プログラム２４とを備える。

【００２２】この入出力装置１０は、キーボードやディスプレイ画面を有して、ユーザとの対話手段となる。記憶装置１１は、暗号化された機密情報を管理する暗号文ファイル３０と、暗号文ファイル３０に対応付けて設けられて、暗号文ファイル３０に格納される機密情報の暗号化に用いた暗号鍵を管理する暗号鍵管理ファイル３１とを備える。ここで、暗号鍵管理ファイル３１に格納される暗号鍵が、更に、自分自身により暗号化されることもあるが、ここでは、説明の便宜上、暗号化されていないことを想定する。

【００２３】消去時間設定プログラム２０は、フロッピィディスクや回線などを介してインストールされて、暗号鍵の消去時間を設定する。設定時間格納域２１は、消去時間設定プログラム２０により設定される消去時間の設定値を格納する。

【００２４】暗号鍵入力消去プログラム２２は、フロッピィディスクや回線などを介してインストールされて、暗号鍵の入力及び消去を実行する。暗号鍵格納域２３は、暗号鍵入力消去プログラム２２により入力される暗号鍵を格納する。

【００２５】暗号復号化プログラム２４は、フロッピィディスクや回線などを介してインストールされて、平文の機密情報を暗号化して暗号文ファイル３０に格納したり、暗号文ファイル３０から暗号化された機密情報を読み出して復号化する。

【００２６】図３に、消去時間設定プログラム２０の実行する処理フローの一実施例、図４に、暗号鍵入力消去プログラム２２の実行する処理フローの一実施例、図５及び図６に、暗号復号化プログラム２４の実行する処理フローの一実施例を図示する。次に、これらの処理フローに従って、本発明について詳細に説明する。

【００２７】消去時間設定プログラム２０は、起動されると、図３の処理フローに示すように、先ず最初に、ステップ１で、設定時間格納域２１に、消去時間のデフォルト値を格納する。

【００２８】続いて、ステップ２で、ユーザから消去時間の設定値が入力されてくるのを待って、消去時間の設定値が入力されてくることを検出すると、ステップ３に進んで、設定時間格納域２１に格納される消去時間のデフォルト値を、ユーザから入力された消去時間の設定値に書き換える。

【００２９】続いて、ステップ４で、ユーザから終了要求が発行されたのか否かを判断して、終了要求が発行されたことを判断するときには、処理を終了し、終了要求が発行されないことを判断するときには、ステップ２に

戻っていくことで、設定時間格納域２１に格納される消去時間の設定値を、ユーザの指定するものに書き換えていく。

【００３０】このようにして、消去時間設定プログラム２０は、ユーザの設定する消去時間の設定値を設定時間格納域２１に格納していくように処理するのである。一方、暗号鍵入力消去プログラム２２は、起動されると、図４の処理フローに示すように、先ず最初に、ステップ１で、ユーザから暗号鍵の入力されてくるのを待って、暗号鍵が入力されてくることを検出すると、ステップ２に進んで、入力されてきた暗号鍵と、暗号鍵管理ファイル３１に管理される暗号鍵とを照合することで、ユーザから入力されてきた暗号鍵が正当なものであるのか否かをチェックする。

【００３１】このステップ２の判断処理に従って、ユーザから入力されてきた暗号鍵が正当なものでないことを判断するときには、その暗号鍵の受け付けを行わずに、そのまま処理を終了する。一方、ユーザから入力されてきた暗号鍵が正当なものであることを判断するときには、ステップ３に進んで、その入力されてきた暗号鍵を暗号鍵格納域２３に格納し、続くステップ４で、設定時間格納域２１に格納される消去時間の設定値を読み取る。

【００３２】続いて、ステップ５で、経過時間を示す変数ｔの値に“０”をセットし、続くステップ６で、計時処理に入って、時間経過に応じて変数ｔの値を順次インクリメントする。続いて、ステップ７で、変数ｔの値がステップ４で読み取った消去時間の設定値に到達したのか否かを判断して、到達していないことを判断するときには、ステップ６に戻って、変数ｔの値のインクリメント処理を続行し、到達することを判断するときには、ステップ８に進んで、暗号鍵格納域２３に格納した暗号鍵を消去（破棄）して処理を終了する。

【００３３】このようにして、暗号鍵入力消去プログラム２２は、ユーザから正当な暗号鍵が入力されてくると、それを暗号鍵格納域２３に格納するとともに、その格納からユーザの設定した消去時間の設定値が経過するときに、その格納した暗号鍵を消去していくように処理するのである。

【００３４】この暗号鍵入力消去プログラム２２の処理に従って、暗号鍵格納域２３には、規定時間の間だけ、ユーザの入力する暗号鍵が保持されることになる。この暗号鍵入力消去プログラム２２の処理を受けて、暗号復号化プログラム２４は、暗号化処理に入るときには、図５の処理フローに示すように、先ず最初に、ステップ１で、ユーザから暗号化指示コマンドの入力されてくるのを待って、暗号化指示コマンドが入力されてくることを検出すると、ステップ２に進んで、暗号鍵格納域２３に暗号鍵が保持されているのか否かを判断する。

【００３５】この判断処理により、暗号鍵格納域２３に

暗号鍵が保持されていることを判断するときには、ステップ３に進んで、その保持されている暗号鍵を使って、ユーザにより編集された平文の機密情報を暗号化して、暗号文ファイル３０に格納する。一方、暗号鍵格納域２３に暗号鍵が保持されていないことを判断するときには、ステップ４に進んで、入出力装置１０に対して暗号化が不可能であることを示すメッセージを出力する。

【００３６】また、復号化処理に入るときには、図６の処理フローに示すように、先ず最初に、ステップ１で、ユーザからファイル表示コマンドの入力されてくるのを待って、ファイル表示コマンドが入力されてくることを検出すると、ステップ２に進んで、暗号鍵格納域２３に暗号鍵が保持されているのか否かを判断する。

【００３７】この判断処理により、暗号鍵格納域２３に暗号鍵が保持されていることを判断するときには、ステップ３に進んで、暗号文ファイル３０に格納される機密情報を読み出し、その保持されている暗号鍵を使って、その読み出した暗号文の機密情報を復号化し、続くステップ４で、その復号化した平文の機密情報をディスプレイ画面に表示する。一方、暗号鍵格納域２３に暗号鍵が保持されていないことを判断するときには、ステップ５に進んで、入出力装置１０に対して復号化が不可能であることを示すメッセージを出力する。

【００３８】このようにして、本発明の情報処理装置１では、ユーザの入力する暗号鍵が暗号鍵格納域２３に一定時間だけ保持され、その後、自動的に消去される構成が採られることで、この暗号鍵が暗号鍵格納域２３に保持されている間は、ユーザは暗号鍵を入力することなく暗号化された機密情報を平文化できるとともに、平文化された機密情報を暗号化できるようになる。

【００３９】図４の処理フローでは、暗号鍵入力消去プログラム２２は、暗号鍵を暗号鍵格納域２３に格納した後、ユーザの設定した消去時間の設定値が経過するときに、その格納した暗号鍵を消去していく構成を採ったが、図７の処理フロー（図４の処理フローと異なる点は、ステップ７ａが設けられている点である）に示すように、入出力装置１０で入力操作が発生する度に、変数ｔの値をリセットしていくことで、入出力装置１０での入力操作が途絶えてから、ユーザの設定した消去時間の設定値が経過するときに、その格納した暗号鍵を消去していく構成を採ってもよい。

【００４０】また、図４の処理フローでは、暗号鍵入力消去プログラム２２は、暗号文ファイル３０に暗号文が既に格納されていることで、暗号鍵管理ファイル３１に暗号鍵が格納されていることを想定して、ユーザから入力される暗号鍵が正当なものであるのか否かをチェックする構成を採ったが、暗号文ファイル３０が作成されていないときには、ユーザから入力される暗号鍵を正当なものと見なして、そのまま暗号鍵格納域２３に格納することになる。この処理に従って、暗号復号化プログラム２４による暗号文ファイル３０の作成が可能になる。

【００４１】次に、図８に従って、本発明について更に詳細に説明する。ここで、図中、４０はファイル操作コマンド、４１は暗号鍵設定部、４２はコマンド制御部、４３はファイル操作制御部、４４は暗号化処理部、４５は暗号鍵保持部、４６は時間設定部である。

【００４２】ファイル操作コマンド４０は、入出力装置１０を介して入力される暗号化指示コマンドや、復号化指示コマンド（上述のファイル表示コマンド）を表している。ここでは、暗号化指示コマンドを“encrypt”、復号化指示コマンドを“decrypt”とする。“encrypt file-name”の入力文字列は、「file-name という名のファイルを暗号化する」ということを意味する。復号化も同様である。この形式で入力されたコマンド名及びファイル名は、コマンド制御部４２に渡されることになる。

【００４３】暗号鍵設定部４１は、暗号鍵の入力を促すコマンドであり、ここでは、“seckey”というコマンド名とする。このコマンド名のみが入力されるときには、暗号鍵を入力するプロンプトを表示することで暗号鍵を入力させ、入力される暗号鍵とこのコマンド名とをコマンド制御部４２に渡すとともに、暗号鍵の入力された時刻を時間設定部４６に渡す。また、“seckey 3600”というように数字付きで入力されたならば、その数字を時間設定部４６に渡す。

【００４４】コマンド制御部４２は、ファイル操作コマンド４０や、暗号鍵設定部４１や、その他のコマンドを受け取り、コマンド名を解析して、“encrypt”／“decrypt”というコマンドであるときには、“encrypt”／“decrypt”と“file-name”とをファイル操作制御部４３に渡し、暗号鍵設定コマンドであるときには、暗号鍵保持部４５に暗号鍵を渡す。

【００４５】ファイル操作制御部４３は、コマンド制御部４２から受け取ったコマンド名と“file-name”とから、暗号化処理部４４を制御して“file-name”を暗号化または復号化する。

【００４６】暗号化処理部４４は、暗号鍵保持部４５に保持される暗号鍵を使って、“file-name”を暗号化または復号化する。暗号鍵保持部４５は、コマンド制御部４２から暗号鍵を受け取ってそれを保持するとともに、時間設定部４６からの暗号鍵破棄指示を受けて、その保持する暗号鍵を破棄する。

【００４７】時間設定部４６は、暗号鍵設定部４１からの時刻を受け取り、その受け取った時点から時間のカウントを行ったり、入出力装置１０を監視して、入出力装置１０の入力操作が途絶えたら時間のカウントを行って、そのカウント値が予め設定された時間に達するときに、暗号鍵保持部４５に対して暗号鍵の破棄を指示する。この処理にあたって、暗号鍵設定部４１から数字を受け取るときには、その数字を秒数として、その秒数の指す時間を暗号破棄を指示するまでの時間として用い

る。

【００４８】このように構成される場合、ユーザは、暗号鍵設定部４１となるコマンド“seckey”を入力する。このようにして起動されると、暗号鍵設定部４１は、“Enter-Key:”プロンプトを表示して、暗号鍵の入力を促す。これを受けて、ユーザは、例えば“ＭＡＤ01772”という暗号鍵を入力する。

【００４９】この暗号鍵の入力を受けて、暗号鍵設定部４１は、コマンド制御部４２に″seckey ＭＡＤ01772″を渡すとともに、入力時点の時刻“97:07:31:12:30(1997年７月31日12時30分）を渡す。

【００５０】これを受けて、コマンド制御部４２は、“seckey”の文字列から、暗号鍵を保持するコマンドと判断し、暗号鍵保持部４５に“ＭＡＤ01772″を渡し、これを受けて、暗号鍵保持部４５は“ＭＡＤ01772″を保持する。

【００５１】次に、暗号文を復号化し平文に変換する動作について説明する。ユーザは、復号化するときには、“decrypt file-name″を入力する。これを受けて、コマンド制御部４２は、復号化指示であると判断して、ファイル操作制御部４３に“decrypt file-name″を渡す。これを受けて、暗号化処理部４４は、暗号鍵保持部４５に暗号鍵が保持されているのか否かをチェックして、保持されているときには、それを使って復号化処理を行い、保持されていないときには、復号化処理を行わない。

【００５２】次に、暗号鍵の破棄処理について説明する。時間設定部４６は、暗号鍵設定部４１から“97:07:31:12:30”を受け取ると、その受け取った時点からデフォルトで設定されている時間（例えば1200秒）をカウントし、その時間が経過するときに、暗号鍵保持部４５に対して暗号鍵の破棄を指示する。このとき、その1200秒経っていない時点で、暗号鍵設定部４１から時刻を受け取ると、その時点から再び1200秒のカウントを開始する。更に、“：”で区切られていない数字（例えば、“3600”）を受け取ると、その時点から3600秒のカウントを開始する。

【００５３】また、別の機能として、時間設定部４６は、暗号鍵設定部４１から“97:07:31:12:30”を受け取ると、入出力装置１０の入力操作の監視を開始して、入力操作が途絶えた時点からデフォルトで設定されている時間（例えば1200秒）をカウントし、その時間が経過するときに、暗号鍵保持部４５に対して暗号鍵の破棄を指示する。このとき、その1200秒経っていない時点で、再び入出力装置１０の入力操作が開始したり、暗号鍵設定部４１から時刻を受け取ると、その時点から再び1200秒のカウントを開始する。更に、“：”で区切られていない数字（例えば、“3600”）を受け取ると、その受け取った時点が入力操作中ならば、次回（入力操作が途絶えて）から3600秒のカウントを開始し、入力操作が途絶えてからのカウント中ならば、その時点から3600秒のカウントを開始する。

【００５４】このようにして、ユーザの入力する暗号鍵が暗号鍵保持部４５に一定時間だけ保持され、その間、ユーザは暗号鍵を入力することなく暗号化された機密情報を平文化できるとともに、平文化された機密情報を暗号化できるようになる。

【００５５】図示実施例に従って本発明を説明したが、本発明はこれに限定されるものではない。例えば、図４の処理フローでは、ユーザから入力されてきた暗号鍵が正当なものであるときに、それを暗号鍵格納域２３に格納する構成を採ったが、正当なものでなくてもそのまま格納してしまう構成を採ってもよい。この構成を採っても、復号化が正規にできないだけで大きな不都合は生じない。

【００５６】

【発明の効果】以上説明したように、本発明の情報処理装置では、ユーザの入力する暗号鍵が一定時間だけメモリに保持され、その後、自動的に消去される構成が採られることで、この暗号鍵がメモリに保持されている間は、ユーザは暗号鍵を入力することなく暗号化された機密情報を平文化できるとともに、平文化された機密情報を暗号化できることから、機密情報の機密性を維持しつつ、操作性の向上を実現できるようになる。

【図面の簡単な説明】

【図１】本発明の原理構成図である。

【図２】本発明の一実施例である。

【図３】消去時間設定プログラムの実行する処理フローである。

【図４】暗号鍵入力消去プログラムの実行する処理フローである。

【図５】暗号復号化プログラムの実行する処理フローである。

【図６】暗号復号化プログラムの実行する処理フローである。

【図７】暗号鍵入力消去プログラムの実行する処理フローである。

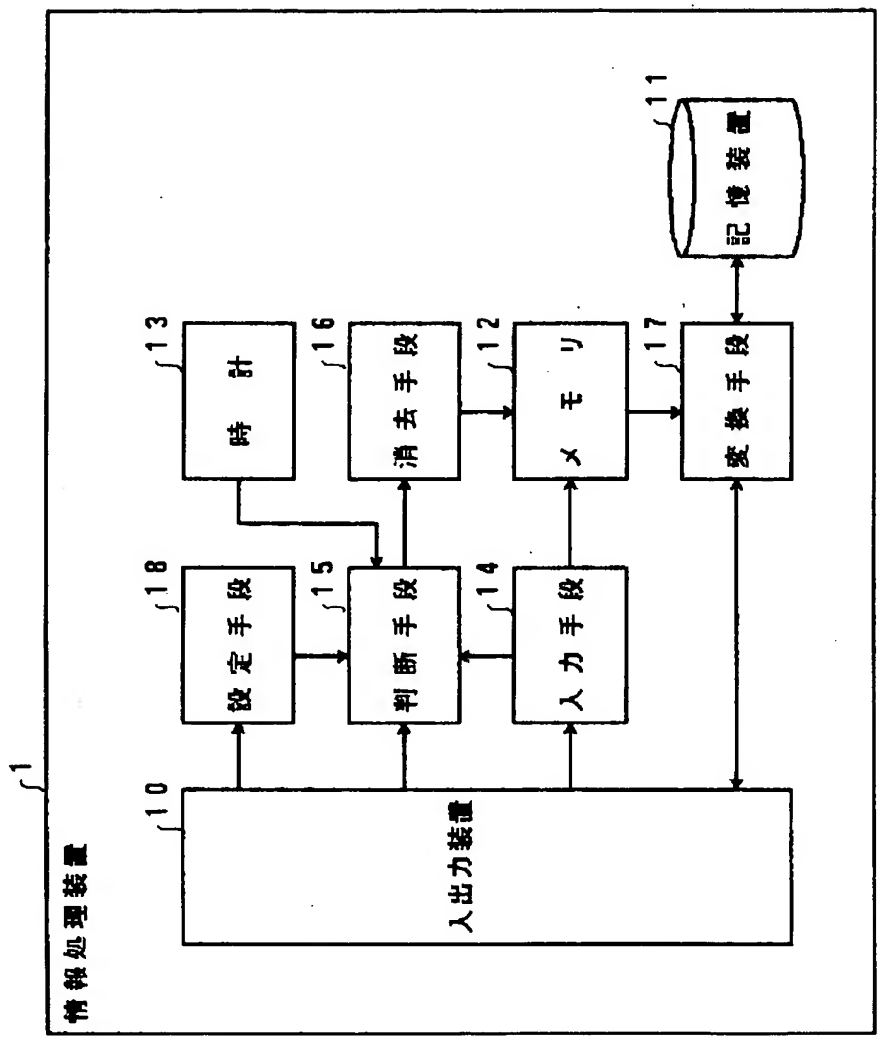
【図８】本発明の一実施例である。

【符号の説明】

１　情報処理装置
１０　入出力装置
１１　記憶装置
１２　メモリ
１３　時計
１４　入力手段
１５　判断手段
１６　消去手段
１７　変換手段
１８　設定手段

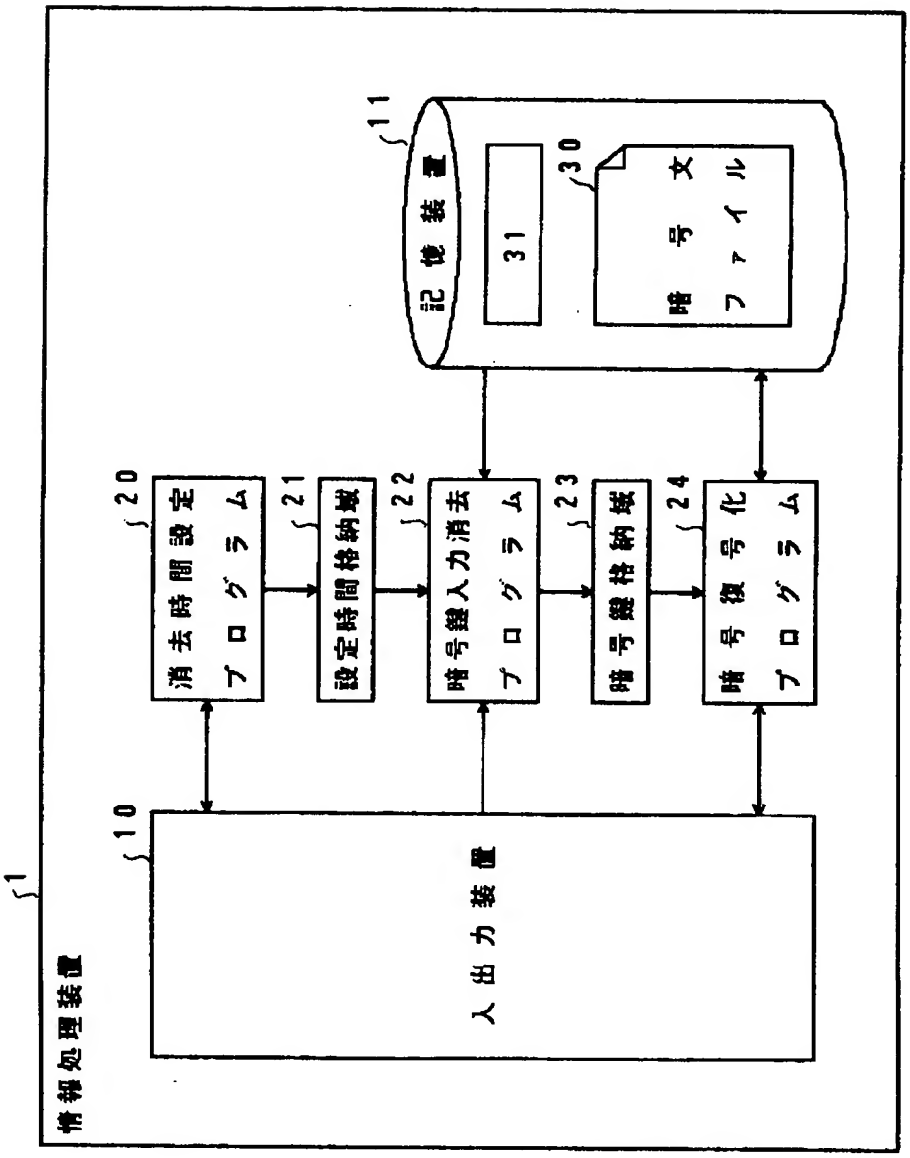
【図１】

本　発　明　の　原　理　構　成　図



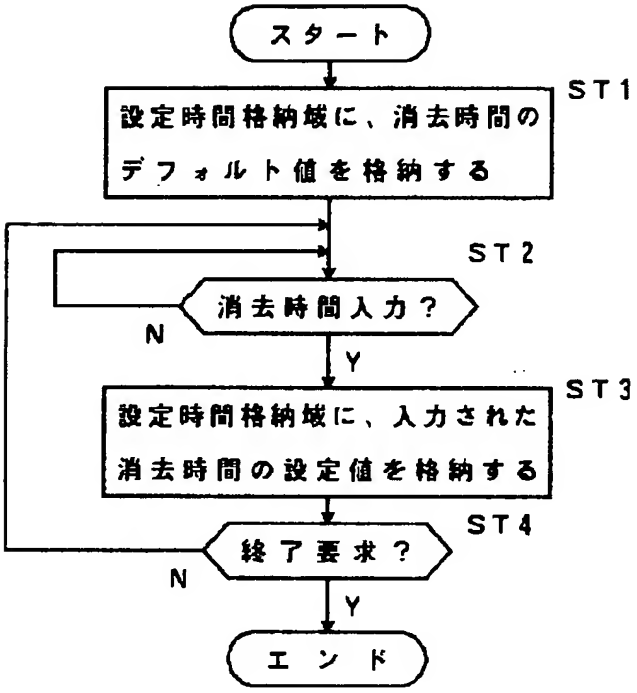
【図２】

本　発　明　の　一　実　施　例


情報処理装置
1
入出力装置
10
記憶装置
11
31
暗号文ファイル
30
消去時間設定プログラム
20
設定時間格納域
21
暗号鍵入力消去プログラム
22
暗号鍵格納域
23
暗号復号化プログラム
24

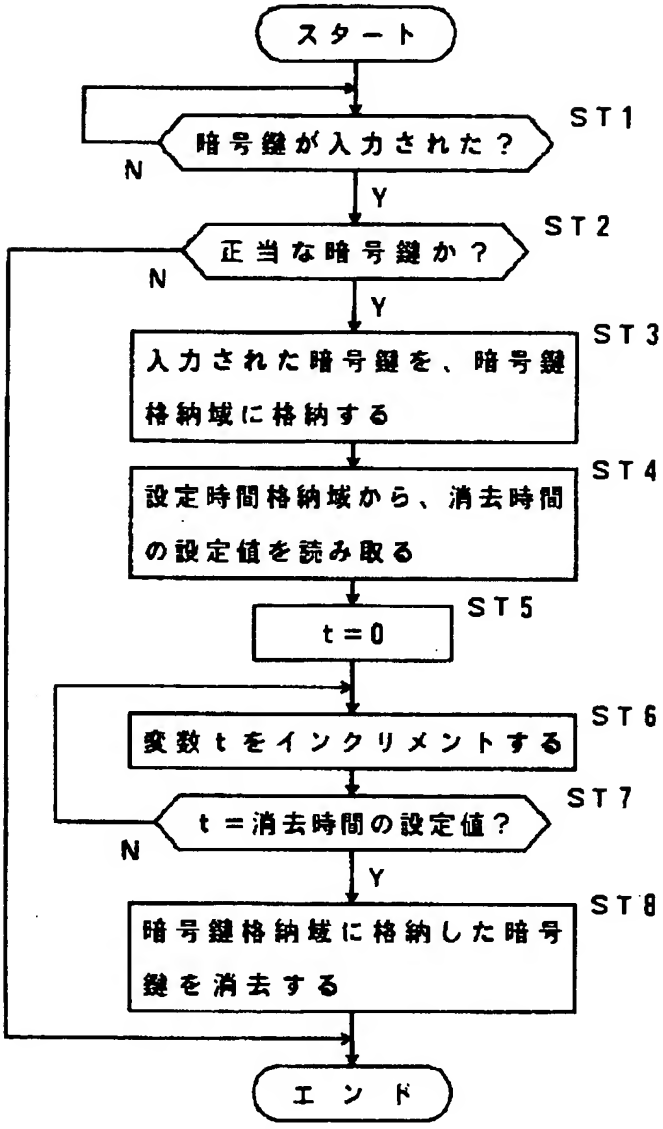
【図３】

消去時間設定プログラムの実行する処理フロー



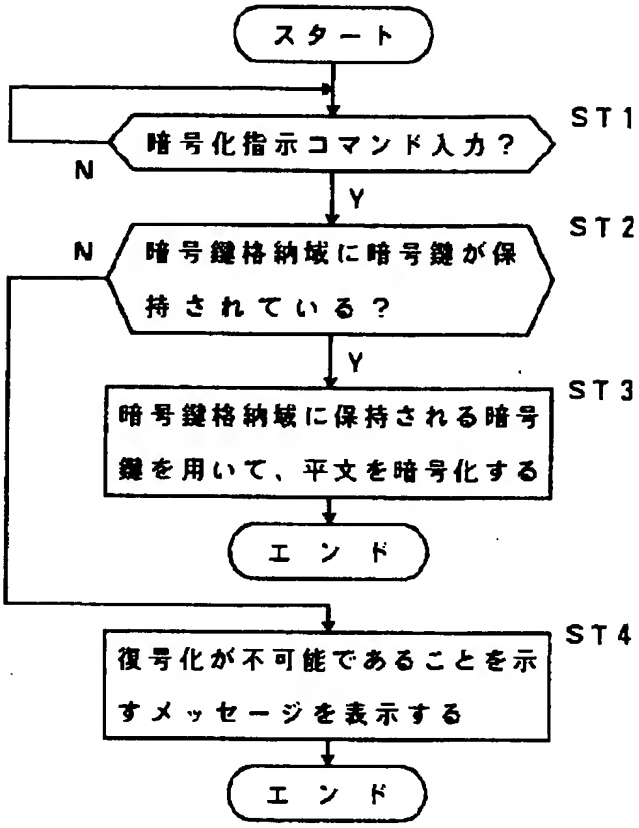
【図４】

暗号鍵入力消去プログラムの実行する処理フロー



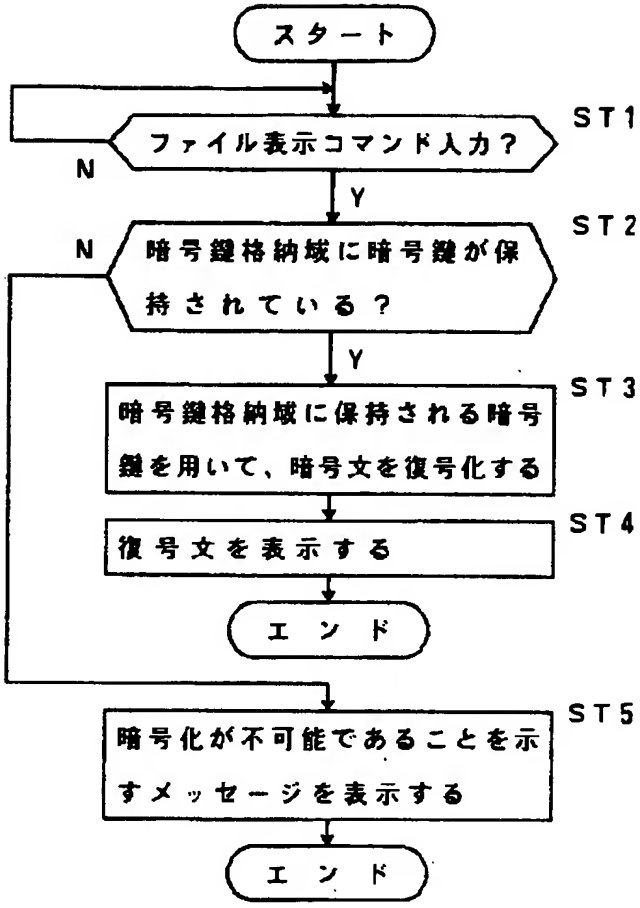
【図５】

暗号復号化プログラムの実行する処理フロー



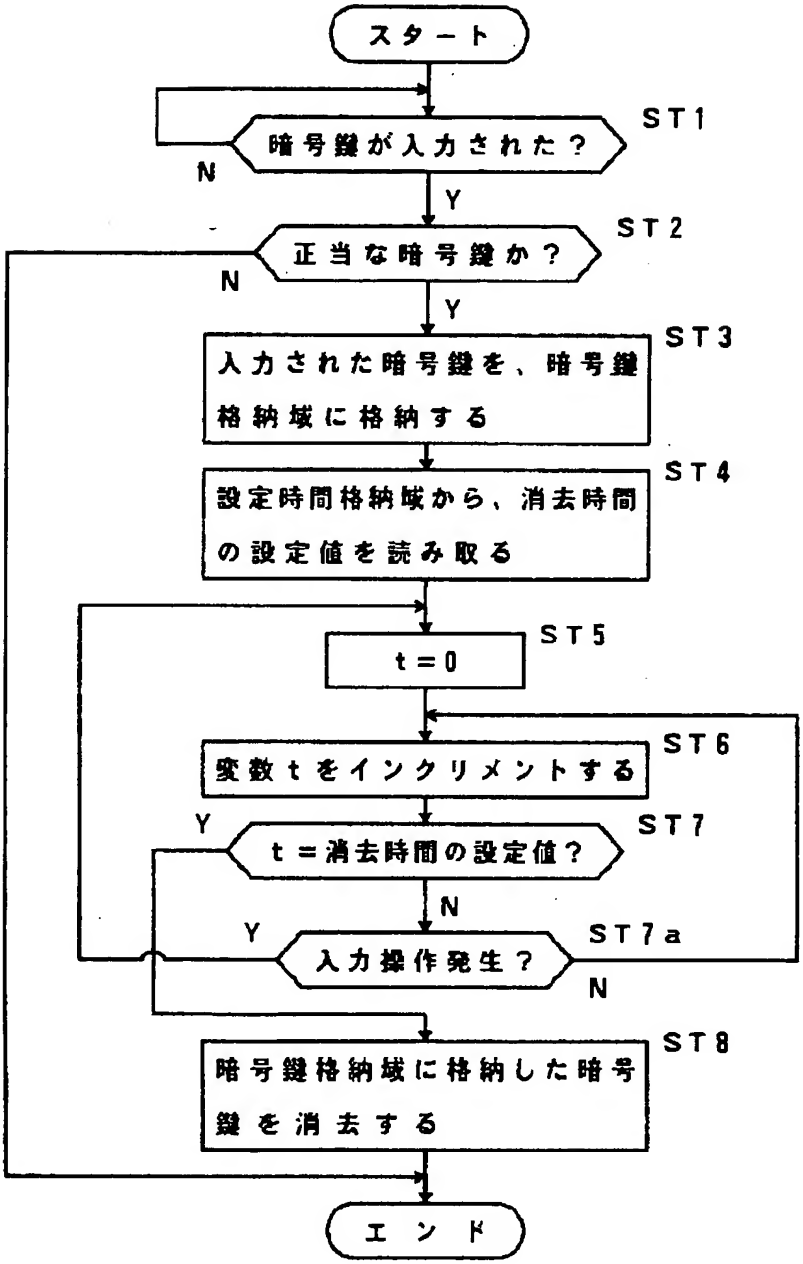
【図６】

暗号復号化プログラムの実行する処理フロー



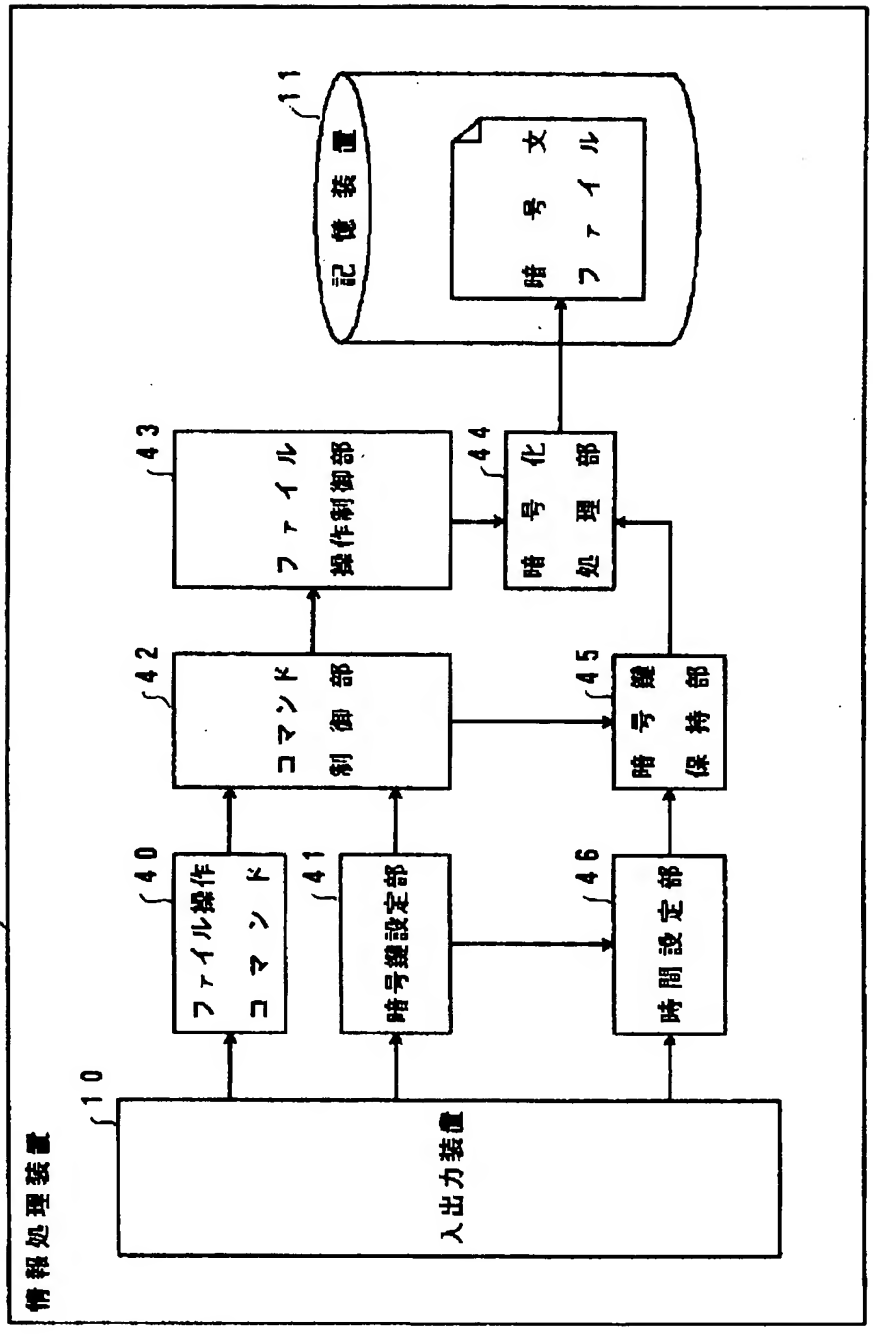
【図７】

暗号鍵入力消去プログラムの実行する処理フロー



【図８】

本発明の一実施例


情報処理装置
1
入出力装置
10
ファイル操作コマンド
40
暗号鍵設定部
41
時間設定部
46
コマンド制御部
42
暗号鍵保持部
45
ファイル操作制御部
43
暗号化処理部
44
記憶装置
11
暗号文ファイル